UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ASHLEY JILEK and LATORRIE GLOVER-BROWN, on behalf of themselves and all others similarly situated, Plaintiffs, v. RETRIEVAL-MASTERS CREDITORS BUREAU, INC. D/B/A AMERICAN MEDICAL COLLECTION AGENCY; QUEST DIAGNOSTICS, INC.; OPTUM360, LLC; AND LABORATORY CORPORATION OF AMERICA HOLDINGS D/B/A LABCORP; Defendants.	Civil Action No. 7:19-cv-5552 **CLASS ACTION COMPLAINT and DEMAND FOR JURY TRIAL**

Plaintiffs Ashley Jilek and LaTorrie Glover-Brown, individually and behalf of all others similarly situated, bring this class action complaint against Retrieval-Masters Creditors Bureau, Inc. d/b/a American Medical Collection Agency ("AMCA"); Quest Diagnostics, Inc.; Optum360, LLC; and Laboratory Corporation of America Holdings d/b/a LabCorp ("LabCorp"); and allege as follows:

INTRODUCTION

1. When people seek medical care, they put their trust not just in the doctors and nurses that care for them, but in the companies that promise to take reasonable precautions to protect their most sensitive information. Defendants Quest Diagnostics and LabCorp and their business associates Optum360 and AMCA violated that trust. Instead of safeguarding their patients' data, Quest Diagnostics, Optum360, and LabCorp provided troves of highly sensitive

information to AMCA—a collections agency with a Better Business Bureau rating of "F" and nearly 600 Consumer Financial Protection Bureau complaints against it—without properly vetting the cybersecurity controls that AMCA had in place to protect that information. AMCA, in turn, neglected to safeguard this data, allowing financially-motivated hackers to steal and sell it on the dark web, a seedy corner of the internet where illicit black markets thrive. Plaintiffs, therefore, bring this suit to recover their losses as a result of Defendants' failure to keep their data secure and to force Defendants to improve their data security practices.

PARTIES

2. Plaintiff Ashley Jilek is an individual residing in Bandera County, Texas, who has used Quest Diagnostics' services and suffered identity fraud.

3. Plaintiff LaTorrie Glover-Brown is an individual residing in Bartow County, Georgia who used both Quest Diagnostics' and LabCorps' services, whose information was compromised in the Data Breach, and who suffered identity fraud.

4. Defendant Retrieval-Masters Creditors Bureau, Inc., d/b/a American Medical Collection Agency, is a New York corporation with its principal place of business in Elmsford, New York.

5. Defendant Quest Diagnostics, Inc. is a Delaware corporation with its principal place of business in Secaucus, New Jersey.

6. Defendant Optum360, LLC, is a Delaware limited liability company with its principal place of business in Eden Prairie, Minnesota.

7. Defendant Laboratory Corporation of America Holdings d/b/a LabCorp is a Delaware corporation with its principal place of business in Burlington, North Carolina.

JURISDICTION AND VENUE

8. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). There are more than 1,000 individual members of the proposed class, their claims exceed the sum or value of $5,000,000, exclusive of interests and costs, and some members of the proposed class are residents of different states than Defendants.

9. This Court has jurisdiction over Defendants because American Medical Collection Agency is a New York corporation, subject to general jurisdiction in New York, because many of the wrongful acts alleged in this Complaint took place in New York, and because the remaining Defendants are registered to conduct business in New York, have sufficient minimum contacts in New York, and intentionally avail themselves of the markets in New York such that the exercise of jurisdiction by this Court is necessary and proper.

10. Venue is proper in this District pursuant to 28 U.S.C. § 1931(b)(3) because the Court has personal jurisdiction over Defendants, a substantial portion of the alleged wrongdoing occurred in this District, and each Defendant has sufficient contacts with this District. Venue is also proper pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims arose in this District.

FACTUAL ALLEGATIONS

11. Quest Diagnostics is a national provider of clinical laboratory services. Among other things, it performs a wide range of diagnostic lab tests for patients and performs drug testing for employers and law enforcement. Quest is a Fortune 500 corporation that made $7.7 billion in revenue in 2017.

12. LabCorp, like its competitor Quest Diagnostics, is a corporation that provides clinical laboratory services. It is one of the largest such companies in the world, and processes 2.5 million lab tests weekly.

13. AMCA, also known as Retrieval-Masters Credit Bureau, is one of the nations' largest debt collectors. It collects debts for direct marketers, telecom companies, toll agencies, and debt buyers across the country. Under the AMCA name, it contracts with laboratories, hospitals, physician groups, and medical providers to recover allegedly unpaid debts from consumers. AMCA purports to be "one of the Nation's top high volume lower balance agencies managing over $1BN in annual receivables for a diverse client base."

14. AMCA states that it is "compliant with all Federal and State Laws and are members of ACA International. We provide our services adhering to the ethical guidelines expected from a National Accounts Receivable Management firm."

15. Despite AMCA's representations that it adheres to industry ethical guidelines, its practices have been the subject of hundreds of consumer complaints. For example, the Consumer Financial Protection Bureau website identifies 699 complaints against Retrieval-Masters and the company is rated "F" by the Better Business Bureau.

16. Defendants Quest Diagnostics, Optum360, and LabCorp are among the companies who directly or indirectly contract with AMCA for debt collection services.

17. Quest contracts with Defendant Optum360, which performs billing services for Quest. Optum360, in turn, subcontracts a portion of the Quest billing services to AMCA. Quest Diagnostics and Optum360 provided AMCA with personal information concerning Plaintiffs and millions of other Quest Diagnostics customers, including their names, dates of birth, Social Security numbers, financial information, and even medical information.

18. LabCorp also provides AMCA with sensitive personal information about its customers, including their name, date of birth, address, phone number, and financial information, and medical information.

AMCA Breach Exposes the Data of 20 Million or More Patients

19. In February 2019, researchers at Gemini Advisory—a company that works with financial institutions to monitor underground markets trafficking in consumer data—found a set of approximately 200,000 credit card numbers being sold on an illicit dark web marketplace. Many of the credit card records were matched with personal information including names, dates of birth, and Social Security numbers. The payment cards appeared to have been compromised between September 2018 and March 2019.

20. Gemini Advisory determined that this financial information originated from a data breach of AMCA's computer networks and notified AMCA. AMCA did not respond. Gemini later contacted law enforcement, which reportedly contacted AMCA directly.

21. Sometime on or before April 8, 2019, AMCA disabled the payment portal suspected of being the hackers' point of entry into AMCA's networks.

22. On May 14, 2019, AMCA notified Quest Diagnostics and Optum360 that the patient data the companies provided to AMCA had been exposed in a data breach. Even though this information was being actively sold on the dark web—and had been for months—none of these companies took prompt steps to notify affected individuals.

23. Weeks later, on June 3, 2019 Quest Diagnostics filed a document with the SEC, explaining that an unauthorized user had accessed an AMCA database containing the information of 11.9 million Quest Diagnostics patients between August 1, 2018 and March 30, 2019. This information "included financial information (e.g., credit card numbers and bank

account information), medical information and other personal information (e.g., Social Security Numbers)."

24. Quest Diagnostics has not indicated how or when it will notify affected the 11.9 million of its customers who are breach victims, stating only that it "will be working with Optum360 to ensure that Quest patients are appropriately notified consistent with the law."

25. On June 4, 2019, LabCorp announced in its own SEC filing that the information of its patients had been exposed in the same breach. The filing stated that unauthorized activity on AMCA's web payment page during the same time period had exposed the first and last name, date of birth, address, phone, date of service, provider, balance information, and credit card or bank account information of LabCorp customers. AMCA believes that the credit card or bank information of at least 200,000 LabCorp customers was accessed. But the data of millions was exposed—7.7 million LabCorp customers have data stored in the insecure AMCA systems.

26. Neither LabCorp nor AMCA have proposed notifying the entirety of the 7.7 million LabCorp customers whose data was compromised. Instead, LabCorp has reportedly begun sending data breach notification letters just to roughly 200,000 of its patients, whose credit or bank account information was accessed.

27. As of result of Defendants' failure to provide notice of the breach, many class members are unaware that their personal information has been compromised and are unaware that they need to take additional steps to protect themselves from identity theft. Many of them already have suffered identity theft that they could have avoided with proper notice. Regardless, every one of the individuals whose information was taken has an increased risk of suffering from identity theft and fraud.

Defendants' Security Practices Are Inadequate

28. Health care providers and their affiliates and vendors frequently are targeted by hackers because their networks store large amounts of sensitive personal information, which they can use to commit identity fraud or sell to other criminals. The threat of data breaches to the healthcare industry has only increased in recent years, as large breaches of health insurers like Anthem, Premera, and Excellus have filled the news. A Raytheon study found that healthcare organizations are twice as likely to suffer a data breach as organizations in other industries.

29. Health care data is especially valuable on the black market, and businesses that store such information are therefore likely to be targeted by cybercriminals. Information maintained by health care companies—such as dates of birth and Social Security numbers—are not easily destroyed and can be used to perpetrate identify theft and other types of fraud even years after the information is stolen. Medical information is highly valuable and is reportedly worth 10 times more than a credit card number on the black market. According to one security expert, a patient's medical records can sell for hundreds of dollars in black market auctions.

30. According to industry experts, "cyber criminals are increasingly targeting the $3 trillion U.S. healthcare industry." Daniel Nutkis, the chief executive of the HITRUST, a healthcare industry cybersecurity organization, stated that "the industry has become, over the last three years, a much bigger target."

31. On April 8, 2014, the FBI issued a Private Industry Notification to healthcare companies, warning that they were likely to be targeted by hackers and that "the possibility of increased cyber intrusions is likely." In August 2014—after Community Health Systems, Inc. experienced a data breach—the FBI also warned U.S. healthcare companies that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting

healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."

32. In 2015, hackers targeted a series of healthcare companies, including Anthem, Premera, and Excellus, leading commentators to label 2015 "the year of the healthcare data breach."

33. While Defendants have provided very little information about how the hackers perpetrated the AMCA data breach, the facts that have been disclosed make clear that AMCA's security was inadequate and Quest Diagnostics, Optum360, and LabCorp failed to adequately vet AMCA's security before providing it with Plaintiff and the class members' personal information. Notably, AMCA's failure to detect the hackers exfiltrating massive amounts of personal information on its own indicates that it failed to adequately monitor its systems for anomalous activity and data flows, which it was required to do under all applicable cybersecurity standards, HIPAA, the GLBA, and numerous other state and federal laws and regulations and private industry standards, like PCI-DSS. Had Defendants ensured AMCA's security controls were reasonable and adequate, the AMCA data breach would not have been successful.

Defendants' Representations to Customers

34. Quest Diagnostics represents to customers in its Notice of Privacy Practices that it is "committed to protecting the privacy of your identifiable health information" in compliance with applicable laws and that it will only disclose protected health information for treatment, payment, healthcare operations, and the necessary use of business associates. It represents that "business associates" that need protected health information are required to maintain the privacy and security of protected health information. Quest Diagnostics also acknowledges that it is required by law to maintain the privacy of patients' protected health information.

35. LabCorp's Notice of Privacy Practices similarly represents that it is "committed to the protection of your PHI and will make reasonable efforts to ensure the confidentiality of your PHI, as required by statute and regulation." LabCorp states that is may disclose protected health information to its business associates, which are "required to maintain the privacy and confidentiality of your PHI."

36. Despite these representations, Quest Diagnostics and LabCorp, and their business associates, Optum360 and AMCA, failed to maintain the privacy and security of patients' protected health information, financial, and personally identifying information.

Defendants Are Subject to Federal and State Laws and Regulations

37. Defendants are covered entities and/or business associates under HIPAA. They are therefore required to comply with the HIPAA Privacy and Security rules, which are designed to protect the privacy and security of patients' protected health information. HIPAA requires them to maintain reasonable and appropriate administrative, technical, and physical safeguards for safeguarding protected health information. They also must take measures to ensure that any business associates with which they share protected health information also take adequate privacy and security measures.

38. Defendants are also subject to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair or deceptive acts or practices in or affecting commerce," as well as the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, *et seq*., which requires them to apply special protections to customers' private data and clearly communicate to customers how they share their sensitive data.

39. Defendants violated each of the aforementioned laws and their implementing regulations by failing to ensure that AMCA's security was adequate to protect the information it stored.

Defendants' Patients and Customers Are Victims

40. As a result of Defendants' deficient security practices and delay in notifying affected individuals, Quest Diagnostics and LabCorp patients and customers are subject to an imminent risk of identity theft that will continue for the foreseeable future. The information Defendants lost is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC"). FTC, About Identity Theft, *available at* http://www.wfm.noaa.gov/workplace/PreventingIdentityTheft_About_Handout_2.pdf.

41. Birthdates and other personally identifying information can be used with Social Security numbers to steal tax refunds and government benefits, assume the victim's identity on social media, prevent victims from obtaining housing and needed medical prescriptions, damage and destroy credit, and even commit crimes in victims' names. More than 17 million Americans had their identities stolen in 2014, costing them over $15 billion. The GAO further reports that victims have "lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft." U.S. Gov't Accountability Office, GAO-14-34, Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent, at 11 (Dec. 2013), *available at* http://www.gao.gov/assets/660/659572.pdf. In 2014, the IRS paid an estimated $3.1 billion in fraudulent tax refunds. *See* U.S. Gov't Accountability Office, GAO-16-589T, IRS Needs to Further Improve Controls Over Taxpayer Data and Continue to Combat Identity Theft Refund Fraud, at 1–2 (Apr. 12, 2016), *available at* http://www.gao.gov/assets/680/676493.pdf.

42. Adding to the damage, the Social Security Administration generally will not assign a replacement social security number absent "harassment, abuse, or life endangerment," and will consider doing so only after "you've done all you can to fix the problems resulting from misuse of your Social Security number, and someone is still using your number[.]" Soc. Sec. Admin., Can I Change My Social Security Number? (Oct. 21, 2016), *available at* https://faq.ssa.gov/link/portal/34011/34019/Article/3789/Can-I-change-my-Social-Security-number; Soc. Sec. Admin., Identity Theft and Your Social Security Number, at 6 (Nov. 2016), available at https://www.ssa.gov/pubs/EN-05-10064.pdf. Even a "new number probably won't solve all your problems," the Social Security Administration reports. "This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number," and "credit reporting agencies use the [old] number to identify your credit record." *Id*. at 7.

43. Finally, because Quest Diagnostics and LabCorp both provided protected health information to AMCA, their patients and customers are likely to become victims of health care identity fraud, a type of identity theft that is particularly expensive and difficult to detect and expensive and time consuming to fix.

44. As a result, Quest Diagnostics patients and customers will have to spend time and money securing their personal information and protecting their identities. They will need to monitor their accounts and credit reports and will have to pay for identity theft protection services credit monitoring or credit reports in the wake of the data breach to prevent or at least quickly detect identity theft using the information taken from AMCA's systems. Those whose payment cards were compromised may have to pay fees to their banks for new debit and credit cards, or have to pay fees to have the cards shipped faster so that they do not have to wait weeks

to make purchases on their accounts. This is particularly true because this payment card information already is being distributed on underground criminal networks.

PLAINTIFF'S EXPERIENCE

45. Plaintiff Ashley Jilek visits Quest Diagnostics at least once per year to have certain diagnostic tests performed. She pays for these tests using her debit card, and Quest Diagnostics keeps her debit card information in its databases. On June 1, 2019, Ms. Jilek discovered that an unknown and unauthorized person had fraudulently charged $500 to the debit card stored in Quest's systems. Had Quest Diagnostics timely informed Ms. Jilek of the data breach, she would have taken immediate action to replace her card and would not have suffered the fraudulent $500 charge. Had Quest Diagnostics revealed that it may share her information with entities that lacked adequate cybersecurity controls, she would not have provided Quest Diagnostics with her debit card information and would have used a different company for her tests.

46. Plaintiff LaTorrie Glover-Brown has used Quest Diagnostics for medical testing on approximately seven occasions. She also has used LabCorp's services. Ms. Glover-Brown disputed the validity of some payments demanded by Defendants. As a result, her accounts with Quest Diagnostics and with LabCorp were sent to collections through AMCA. In addition, Ms. Glover-Brown paid for the services performed by Quest Diagnostics and LabCorp using her payment cards. In April 2019, Ms. Glover-Brown discovered that she had been a victim of identity fraud. In early June 2019, Ms. Glover-Brown received a notification letter from AMCA, informing her that she is one of the LabCorp data breach victims. Had Quest Diagnostics or LabCorp revealed that they may share her information with entities that lack adequate

cybersecurity controls, she would not have provided them with her payment card information and would have used different companies for her tests.

CLASS ALLEGATIONS

47. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of herself and the classes preliminary defined as:

> ***Nationwide Class****:* All individuals in the United States whose personal information was provided to AMCA by Quest Diagnostics, Optum360, and/or LabCorp and was compromised as a result of the AMCA data breach.

> ***Texas Subclass***: All individuals residing in Texas whose personal information was provided to AMCA by Quest Diagnostics, Optum360, and/or LabCorp and was compromised as a result of the AMCA data breach.

48. Excluded from the proposed classes are Defendants; any affiliate, parent, or subsidiary of Defendants; any entity in which Defendants have a controlling interest; any officer, director, or employee of Defendants; any successor or assign of Defendants; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

49. Plaintiffs satisfy the numerosity, commonality, typicality, and adequacy prerequisites for suing as a representative party pursuant to Rule 23.

50. **Numerosity**. The proposed classes consist of millions of individuals who had their information accessed in the AMCA breach, making joinder of each individual class member impracticable.

51. **Commonality**. Common questions of law and fact exist for the proposed classes' claims and predominate over questions affecting only individual class members. Common questions include:

a. Whether Defendants owed a duty to Plaintiffs and members of the proposed classes to take reasonable measures to safeguard their personal information;

b. Whether Defendants knew or should have known that their and their business associates' systems were inadequate and susceptible to a data breach;

c. Whether Defendants breached their legal duties in allowing their cybersecurity systems to be compromised;

d. Whether Defendants owed a duty to Plaintiff and members of the proposed classes to provide timely and adequate notice of the data breach;

e. Whether Defendants breached their contractual promises to adequately protect class members' personal information;

f. Whether Defendants' failure to implement adequate security controls violate applicable state consumer protection laws;

g. Whether class members may obtain damages, restitution, declaratory, and injunctive relief against Defendants; and

h. What security procedures and data-breach notification procedure Defendants should be required to implement as part of any injunctive relief ordered by the Court.

52. **Typicality**. Plaintiffs' claims are typical of the claims of the proposed classes because, among other things, Plaintiffs and class members sustained similar injuries as a result of Defendants' uniform wrongful conduct and their legal claims all arise from the same core data breach and business practices of Defendants.

53. **Adequacy**. Plaintiffs will fairly and adequately protect the interests of the classes. Their interests do not conflict with class members' interests and they have retained counsel experienced in complex class action and data privacy litigation to vigorously prosecute this action on behalf of the classes.

54. In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual class members and a class action is superior to individual litigation. The amount of damages available to individual plaintiffs is insufficient to make litigation addressing Defendants' conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

55. Certification of the class is also appropriate pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), and/or (c)(4).

FIRST CAUSE OF ACTION

NEGLIGENCE

(On Behalf of the Nationwide Class Against All Defendants)

56. Plaintiffs incorporate the above allegations as if fully alleged herein.

57. Defendants owed a duty to Plaintiffs and class members to exercise reasonable care in obtaining, retaining, deleting, securing, and protecting their personal information from being compromised, lost, stolen, accessed, or misused by unauthorized persons. More

specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendants' security systems to ensure that Plaintiffs' and class members' personal information was adequately secured and protected; (b) implementing adequate and effective processes to detect an intrusion into their information systems in a timely manner; (c) timely acting upon warnings and alerts, including those generated by their own security systems, regarding network intrusions; and (d) maintaining data security measures at least consistent with industry standards.

58. Defendants' duty to use reasonable care arose from several sources, including those described below.

59. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and class members were the foreseeable and probable victims of Defendants' inadequate security practices. Not only was it foreseeable that Plaintiffs and class members would be harmed by the failure to protect their personal information (because hackers routinely attempt to steal such information and use it for nefarious purposes), Defendants knew Plaintiffs and the class members probably would be harmed.

60. Defendants duty to safeguard Plaintiffs' and the class members' personal information is also buttressed by HIPAA, which was enacted to protect individuals from improper disclosure of their personal information through inadequate data security.

61. Defendants also had duties to safeguard the personal information of Plaintiffs and class members and to promptly notify them of a breach under other laws and regulations that require Defendants to reasonably safeguard sensitive personal information, including Section 5 of the FTC Act, the Gramm-Leach-Bliley Act, and state data security and data breach notification statutes.

62. Defendants also had a pre-existing duty to exercise reasonable care to safeguard Plaintiffs' and class members' personal information, which extends to those to which Defendants directly or indirectly provided such information.

63. Defendants also had a duty to timely notify Plaintiffs and class members of the data breach, so they could take appropriate prophylactic and mitigation measures, including freezing their credit, purchasing adequate identity theft protection products, monitoring their accounts even more carefully for unauthorized charges, and cancelling or changing usernames and passwords for compromised accounts,

64. Defendants breached the duties they owed to Plaintiffs and class members described above and thus were negligent. Defendants breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the Plaintiffs' and class members' personal information; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiffs' and the class members' personal information in Defendants' possession had been or was reasonably believed to have been, stolen or compromised.

65. Plaintiffs' and class members' personal information would not have been compromised but for Defendants' wrongful and negligent breach of their duties.

66. As a direct and proximate result of Defendants' negligence, Plaintiffs and class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and statutory damages, in an amount to be proven at trial. Plaintiffs' and class members' injuries include: costs stemming from the use of their personal information and the diminution in its value as a result of the Data Breach; costs associated with the detection and

prevention of identity theft, including purchasing credit monitoring and identity theft protection services; costs related to the loss of use of and access to their funds; adverse effects on their credit; costs associated with time spent and the loss of productivity from addressing the actual and future consequences of the Defendants' data breach; continued risk of exposure to hackers and thieves of their personal information, which remains in Defendants' inadequately secured systems; and the diminution of the value and/or loss of the benefits of products and services purchased directly or indirectly from Defendants.

SECOND CAUSE OF ACTION

NEGLIGENCE PER SE

(On Behalf of the Nationwide Class Against All Defendants)

67. Plaintiffs incorporate the above allegations as if fully alleged herein.

68. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission, the unfair act or practice by companies such as Defendants of failing to use reasonable measures to protect personal information. Various FTC publications and orders also form the basis of Defendants' duties.

69. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect personal information and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of personal information they obtained and stored and the foreseeable consequences of a data breach.

70. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

71. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

72. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the class.

73. As a direct and proximate result of Defendants' negligence, Plaintiffs and class members have been injured, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION

UNJUST ENRICHMENT

(On Behalf of the Nationwide Class Against All Defendants)

74. Plaintiffs incorporate the above allegations as if fully alleged herein.

75. Plaintiffs and class members have an interest, both equitable and legal, in the personal information about them that was conferred upon, collected by, and maintained by Defendants and that was ultimately stolen in the data breach. This personal information was conferred on Defendants directly by Plaintiffs and class members.

76. Defendants were benefitted by the conferral upon them of Plaintiffs' and class members' personal information and by their ability to retain and use that information. Defendants understood that they were in fact so benefitted.

77. Defendants also understood that the personal information pertaining to Plaintiffs and class members was private and confidential and its value depended upon Defendants' maintaining the privacy and confidentiality of that personal information.

78. But for Defendants' commitment to maintain the confidentiality and security of their personal information, Plaintiffs and the class members would not have permitted Defendants to obtain their personal information.

79. As a result of the wrongful conduct alleged herein, Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and class members. Among other things, Defendants continue to benefit and profit from the use of the Plaintiffs' and class members' personal information, while its value to Plaintiffs and class members has been diminished.

80. Under the doctrine of unjust enrichment, it is inequitable for Defendants to be permitted to retain the benefits they received, and are still receiving, without justification, from Plaintiffs and class members in an unfair and unconscionable manner. Defendants' retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

81. The benefits conferred upon, received, and enjoyed by Defendants were not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendants to retain the benefits.

82. Defendants are therefore liable to Plaintiffs and class members for restitution in the amount of the benefit conferred on Defendants as a result of their wrongful conduct, including specifically the value to Defendants of the personal information that was stolen in the Defendants' data breach and the resulting profits Defendants received and are receiving from the use of that information.

FOURTH CAUSE OF ACTION

BREACH OF CONTRACT

(On Behalf of the Nationwide Class Against Defendants Quest Diagnostics and LabCorp)

83. Plaintiffs incorporate the above allegations as if fully alleged herein.

84. Plaintiffs and class members entered into agreements with Quest Diagnostics that it would provide them with medical services in exchange for the consideration of monetary payment.

85. Ms. Glover-Brown and class members entered into agreements with LabCorp that it would provide them with medical services in exchange for the consideration of monetary payment.

86. Plaintiffs and class members fully performed their obligations under the contracts with Defendants.

87. Defendants Quest Diagnostics and LabCorp breached their agreements with Plaintiffs and class members by failing to protect their personal information. Specifically, they (1) failed to take reasonable steps to ensure that their contractors AMCA and/or Optum360 used safe and secure systems to protect that information; (2) failed to ensure that their contractors had appropriate security protocols and measures in place to protect that information; (3) allowed their contractors to disclose that information to unauthorized third parties; and (4) failed to promptly alert or give notice of the breach to Plaintiffs and class members.

88. As a direct and proximate result of Defendants' breaches of contract, Plaintiffs and class members sustained actual losses and damages as described in detail above.

FIFTH CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT

(On Behalf of the Nationwide Class Against Defendants Quest Diagnostics and LabCorp)

89. Plaintiffs incorporate the above allegations as if fully alleged herein.

90. Plaintiffs and class members entered into implied contracts with Defendants Quest Diagnostics and LabCorp when they obtained health care services from these Defendants.

91. As part of these transactions, Defendants Quest Diagnostics and LabCorp agreed to safeguard and protect the personal information of Plaintiffs and class members and to timely and accurately notify them if their personal information was breached or compromised.

92. Plaintiffs and class members entered into the implied contracts with the reasonable expectation that Defendants' would ensure that they only provided personal information to contractors with adequate data security practices and policies.

93. Plaintiffs and class members would not have obtained Quest Diagnostics' and LabCorp's health care services or provided and entrusted their personal information to Defendants, in the absence of the implied contract or implied terms between them and Defendants. Safeguarding Plaintiffs' and class members' personal information and providing prompt and sufficient data breach notification was critical to realizing the intent of the parties.

94. Plaintiffs and class members fully performed their obligations under the implied contracts with Defendants.

95. Defendants Quest Diagnostics and LabCorp breached their implied contracts with Plaintiffs and class members when they (1) failed to have security protocols and measures in place to protect that information; (2) disclosed that information to unauthorized third parties; and

(3) failed to provide timely and accurate notice that Plaintiffs' and class members' personal information was compromised as a result of the data breach.

96. As a direct and proximate result of Quest Diagnostics' and LabCorp's breaches of implied contract, Plaintiffs and class members sustained actual losses and damages as described in detail above.

SIXTH CAUSE OF ACTION

NEW YORK GENERAL BUSINESS LAW, N.Y. GEN. BUS. LAW § 349, et. seq.

(On Behalf of the Nationwide Class Against AMCA)

97. Plaintiffs incorporate the above allegations as if fully alleged herein.

98. AMCA engaged in deceptive acts or practices in the conduct of its business, trade, and commerce, or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and class members' personal information, which was a direct and proximate cause of the AMCA data breach;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the GLBA, 15 U.S.C. § 6801, et seq., which was a direct and proximate cause of the Defendants data breach;

c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and class members' personal information, including by implementing and maintaining reasonable security measures;

d. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and class members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the GLBA, 15 U.S.C. § 6801, et seq.;

e. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and class members' personal information; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the GLBA, 15 U.S.C. § 6801, et seq.

99. AMCA's representations and omissions were material because they were likely to deceive reasonable consumers as well as companies who retained AMCA, including Quest Diagnostics and LabCorp, about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' personal information.

100. AMCA acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiffs' and class members' rights.

101. As a direct and proximate result of AMCA's deceptive and unlawful acts and practices, Plaintiffs and class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for

fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of the benefit of their bargains with Defendants; and loss of value of their personal information.

102. AMCA's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including hundreds of thousands of New Yorkers affected by the Defendants' data breach.

103. The above deceptive and unlawful practices and acts by AMCA caused substantial injury to Plaintiffs and class members that they could not reasonably avoid.

104. Plaintiffs and class members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

SEVENTH CAUSE OF ACTION

DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT, Texas Bus. & Com. Code §§ 17.41, *et seq.*

(On Behalf of Plaintiff Glover-Brown and the Texas Sub-Class Against All Defendants)

105. Plaintiffs incorporate the above allegations as if fully alleged herein.

106. Defendants are "persons," as defined by Tex. Bus. & Com. Code § 17.45(3).

107. Ms. Glover-Brown and the Texas Subclass members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

108. Defendants engaged in trade or commerce within the meaning of Tex. Bus. & Com. Code § 17.45(6), in that they engaged in trade and commerce that directly and indirectly affected the people of Texas, and they advertised, offered for sale, sold, leased, or distributed goods or services within the meaning of the statute.

109. Defendants engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

a. Causing confusion or misunderstanding as to the certification of goods or services;

Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another; and advertising goods or services with intent not to sell them as advertised;

c. Advertising goods or services with intent not to sell them as advertised;

d. Failing to disclose information concerning goods or services which was known at the time of the transaction where such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.

110. Defendants false, misleading, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Ms. Glover-Brown's and Texas Subclass members' personal information, which was a direct and proximate cause of the Defendants data breach;

b. Failing to identify foreseeable security and privacy risks, which was a direct and proximate cause of the data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Ms. Glover-Brown's and Texas Subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the data breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Ms. Glover-Brown's and Texas Subclass members' personal information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Ms. Glover-Brown's and Texas Subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801, et seq., and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Ms. Glover-Brown's and Texas Subclass members' personal information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Ms. Glover-Brown's and Texas Subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801, et seq., and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

111. Defendants intended to mislead Ms. Glover-Brown and Texas Subclass members and induce them to rely on their misrepresentations and omissions.

112. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' personal information.

113. Ms. Glover-Brown and the Texas Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

114. Defendants had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and amount of personal information in their possession, and the generally accepted professional standards in the industry. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Ms. Glover-Brown and the Texas Subclass, and Defendants because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from their:

a. Possession of exclusive knowledge regarding the security of the data in their systems;

b. Active concealment of the state of their security controls; and/or

c. Incomplete representations about the security and integrity of their computer and data systems, while purposefully withholding material facts from Ms. Glover-Brown and the Texas Subclass that contradicted these representations.

115. Defendants engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Defendants engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

116. Consumers, including Ms. Glover-Brown and Texas Subclass members, lacked knowledge about deficiencies in Defendants' data security because this information was known exclusively by Defendants. Consumers also lacked the ability, experience, or capacity to secure the personal information in Defendants' possession or to fully protect their interests with regard to their data. Ms. Glover-Brown and Texas Subclass members lack expertise in information security matters and do not have access to Defendants' systems in order to evaluate its security controls. Defendants took advantage of their special skill and access to personal information to hide their inability to protect the security and confidentiality of Ms. Glover-Brown's and Texas Subclass members' personal information.

117. Defendants intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Defendants' conduct is glaringly noticeable, flagrant, complete, and unmitigated. The data breach, which resulted from Defendants' unconscionable business acts and practices, exposed Ms. Glover-Brown and Texas Subclass members to a wholly unwarranted risk to the safety of their personal information and the security of their identity and credit, and worked a substantial hardship on a significant and unprecedented number of consumers. Ms. Glover-Brown and Texas Subclass members cannot mitigate this unfairness because they cannot undo the data breach.

118. Defendants acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Ms. Glover-Brown's and Texas Subclass members' rights.

119. As a direct and proximate result of Defendants' unconscionable and deceptive acts or practices, Ms. Glover-Brown and Texas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of the benefits of their bargains with Defendants; and loss of value of their personal information. Defendants' unconscionable and deceptive acts or practices were a producing cause of Ms. Glover-Brown's and Texas Subclass members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish.

120. Defendants' violations present a continuing risk to Ms. Glover-Brown and Texas Subclass members as well as to the general public.

121. Ms. Glover-Brown and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and behalf of the proposed classes, pray for the following relief:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the class as requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiffs are proper representatives of the class;

B. Declaratory relief, declaring Defendants' actions unlawful;

C. Injunctive relief, including an order requiring Defendants to implement and maintain technical and administrative security controls that are appropriate for the type and amount of data they maintain and to immediately provide reasonable notice to all individuals whose information was compromised in the AMCA data breach.

D. Damages, including where appropriate, statutory and punitive damages, restitution, attorneys' fees, costs, and such other and further relief as is just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all issues in this action so triable of right.

DATED: June 14, 2019

Respectfully submitted,

/s/ John A. Kehoe

John A. Kehoe (JK-4589)
KEHOE LAW FIRM, P.C.
41 Madison Avenue, 31st Floor
New York, NY 10010
(212) 804-7700
jkehoe@kehoelawfirm.com

Eric H. Gibbs
David M. Berger
GIBBS LAW GROUP, LLP
501 14th Street, Suite 1110
Oakland, CA 94612
(510) 350-9700
ehg@classlawgroup.com
dmb@classlawgroup.com

Counsel for Plaintiffs and the Proposed Class